

# Project: forge a signature to pretend that you are Satoshi

代码说明：首先是 ECDSA 签名算法的代码，接下来利用课件的方法编写代码对 Satoshi 的签名进行伪造，假设已知他的一个签名，之后可在不知晓他私钥的前提下伪造出一个对 e' 的签名 (r',s')。具体代码则将课件数学式子转化为代码即可。

运行说明：直接运行 py 文件

运行结果：

```
Satoshi持有的私钥为： 9588701486067903007972542880253404164
Satoshi对 'sdu hello' 的签名为： (3140883959917274975856699884658540524, 27313888972103203347607676663995428789)
对Satoshi的签名进行验证-----
验证通过！

-----接下来对Satoshi签名进行伪造，以下过程均不知道Satoshi的私钥d-----
伪造签名信息的哈希为：10538007220899772315562626464558589908
伪造的签名为： (17563345368166287192604377440930983180, 3512669073633257438520875488186196636)
接下来对伪造签名进行验证-----
验证通过！
```